References

American Society for Industrial Security (ASIS) Online Security News and information, ASIS Press Releases, May 10, 1998 “ASIS Releases Complete Special Report on Intellectual Property Loss and Economic/Industrial Espionage” (Detailed summary of statistics cited in the “ASIS 1997/1998 Trends in Intellectual Property Loss Survey Report, May 10, 1998.”)

American Electronics Association, "Cyberstates, v. 3.0", Washington, DC, 1999.

Angelica, Amara D., "Batten Down the Hatches", *Silicon Valley TechWeek*, 1998

Bailey, Lee. "Record Industry Losing Millions to Bootleggers", *EUR/Electronic Urban Report*, April 9, 1999; (http://www.EURweb.com/, April 9, 1999)

Becker, David, "Ripped Off", *Silicon Valley TechWeek*, May 3, 1999, p. 1

Bell Atlantic, “Bell Atlantic Calls for Industry Cooperation to 'Outfox' $4-Billion-a-Year Phone Fraud”, News Release, March 3, 1997.

Bernstein, Jodie, Director of the Bureau of Consumer Protection, Federal Trade Commission, Prepared Statement of the Federal Trade Commission on Financial Identity Theft, Before the Subcommittee on Telecommunications, Trade, and Consumer Protection, and the Subcommittee on Finance and Hazardous Materials of the Committee on Commerce, United States House of Representatives, Washington, D.C., April 22, 1999.

Burey, Joe, "Lack of Clear-Cut Jurisdiction Over Internet Seen Creating Conflict", Inside Washington Publishers, June 18, 1999

Business Software Alliance (BSA), "Worldwide Business Software Piracy Losses Estimated At Nearly $11 Billion In 1998, Annual Study Finds More Than One-Third of Applications Are Pirate Copies”, Press Release, Washington, DC, May 25, 1999

Business Software Alliance (BSA), "Five Southern California Organizations Settle Software Copyright Claims" (press release), February 24, 1999.

C&R Research, "1998 Study of Cable Signal Theft: California", California Cable Television Association, June 1999.

Carter, David and Andra Katz, "Trends and Experiences in Computer-Related Crime: Findings from a National Survey", presented at th Annual Meeting of Criminal justice Sciences. March 15, 1996.

Cellular Telecommunications Industry Association (CTIA), "Frequently Asked Questions and Fast Facts" *WOW-COM, The World of Wireless Communications Consumer Resources*,, (1997/1998)

Clausing, Jeri, "Software Piracy Costs U.S. Billions, Senate Panel is Told", The New York Times, April 30, 1999.

Computer Security Institute, "1999 CSI/FBI Computer Crime and Security Survey", San Francisco, March 1999. CSI also published similar surveys in 1997 and 1998.

"Study Finds Computer Virus Costs to Business Surging", Reuters, June 18, 1999, Computer Economics study of 185 companies representing 900,000 international users

Dalton, Gregory, "Acceptable Risks", *Information Week*, (698), Aug. 31, 1998.

Dertouzos, James N., Eric V. Larsen and Patricia A Ebener, "The Economic Costs and Implications of High-Technology Hardware Theft", Rand Corp., Santa Monica, 1999.

"Digital Music Standard Raises Host of Questions", New York Times, June 30, 1999

Ernst & Young Industrial Fraud Group, "Fraud: The Unmanaged Risk", May 1996.

Eyres, William E., "Putting the Brakes on Information Age Crime", *The Police Chief*, June 1999.

Farmer, Dan, "Shall We Dust Moscow?", Internet Security Survey, Dec. 1996 (http://www.fish.com/survey/)

Fisse, Brent and Peter Leanard, "Internetional Electronic Money Systems and Money Laundering", presented at the ASC Electronic Commerce Conference, Sydney, February 4, 1999

Fitzpatrick, Eileen, "Studios File Piracy Suit" *Billboard*, April 24, 1999

Freeh, Louis J., Director Federal Bureau of Investigation before the Senate Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies", Washington, D.C., March 10, 1998.

Gallagher, Neil J., Deputy Assistant Director, Criminal Division, Federal Bureau of Investigation, "Testimony before the Congressional Joint Economic Committee, Washington, D. C., March 24, 1998.

Hines, Matt, “Microsoft Finds First Counterfeit OEM Windows 98 Copies”, Newsbytes News Network, A division of Post-Newsweek Business Information, Inc., Nov. 12, 1998.

Holland, Bill, "RIAA Piracy Picture Mixed", Billboard, April 17, 1999.

Hopkins, Nick, "Hi-Tech Policing Urged to fight Internet Crime", *The Guardian*, Manchester, June 24, 1999

Information Week, "Network Protection Tools", describes a Zona Research Study of 359 IT Managers, May 31, 1999, p. 112

Kabay, M. E., "ICSA White Paper on Computer Crime Statistics", ICSA, On-going, last modified, November 19, 1998.

Lawrence, Steve and C. Lee Giles, "How Big is the Web", NEC Research Institute, April 1998 (http://www.neci.nj.nec.com/homepages/lawrence/websize.html)

Lawrence, Steve and C. Lee Giles, "Accessibility of Information on the Web", Nature, v100(8), July 1999

Lewis, Brian C., "Information Warfare" (http://www.fas.org/irp/eprint/snyder/infowarfare.htm)

Louis Harris and Associates, *Consumers in the 21st Century*, for the National Consumers League, May 21, 1999

Meyer, J. F., C. Short, "Investigating Computer Crime: Concerns Voiced by Local Law Enforcement Agencies", *The Police Chief*, v. 65 (5), May 1998, 28-30.

Microsoft Corporation, Inc., "The Scope and Impact of Software Piracy and Counterfeiting on California: The Prevalence of Criminal Counterfeiting Operations in the Nation's High Tech Center", Redmond, WA, 1999.

Miller, Greg, "Firms Say Hackers Cost Them $291Million", *Los Angeles Times*, May 3, 1999.

Mitchell, Stevan D., and Elizabeth A Banker, " Private Intrusion Response", *Harvard Journal of Law and Technology*, v 11, Cambridge, Spring 1998.

Morgester, Robert M., "Creating and Funding a High Technology Crime Task Force, Prosecutor's Brief, vol. xxi (1), California District Attorneys Quarterly Journal, Sacramento, 1999.

MPAA (Motion Picture Association of America), private communication, May 1999.

Multichannel Online, "CTAM Researches Cable-Theft Attitudes", 5/20/99

National Counterintelligence Center, "National Counterintelligence (CI) Needs Survey", *Counterintelligence and Developments, News Trends and Analysis on CI and Security Issues,* June 1998.

National Fraud Information Center,"1998 Telemarketing Fraud Statistics", February 27, 1999.

Nevada Office of the Attorney General, "Nevada High Technology Crime Task Force: A Strategic Plan to Combat High Technology Crime in California, January, 1997.

Ohlhausen, Peter E., "Combating High-Tech Crime in California: The Task Force Approach", for the California High-Tech Task Force Committee, June 1997.

Owens, Charles L., Chief, Financial Crimes Section, Federal Bureau of Investigation, "Testimony before the Subcommittee on Technology, Terrorism, and Governmental Information, Committee on the Judiciary, United States Senate, Washington, D. C., March 19, 1997

Parker, Donn, *Fighting Computer Crime*, Wiley, New York, 1998.

Power, Richard, "Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare", Computer Security Institute, San Francisco, CA, 1998.

Radcliffe, Deborah, "Handling Crime in the 21st Century", CNN Interactive, Dec. 15, 1998.

Rosenblatt, Kenneth S., *High Technology Crime*, KSK Publications, San Jose, 1995

Spafford, Gene, "Testimony Before the Computer and Network Security Hearing", Subcommittee on Technology, US House of Representatives Committee on Science, Feb. 11, 1997.

Starback, Tim, Director of Marketing, Émigré, Inc., on behalf of Software Information Industry Association (SIIA), Testimony Before the Subcommittee on Courts and Intellectual Property, House Judiciary Committee, Oversight Hearing on Implementation of the Net Act and Enforcement Against Internet Piracy, May 12, 1999."

Swartwood, Dan T. , and Richard J. Hefferman, "Trends in Intellectual Property Loss: Major Findings of the 1997 ASIS Intellectual Property Loss Survey", American Society for Industrial Security, Alexandria, VA, March 1998.

Telecom and Network Security Review, "Toll Fraud Rising in 1997 to More than $4 billion", v, 5(4), April 1997.

Tillett, L. Scott, "Title - check", Federal Computer Week / CNN, June 1, 1999.

Vatis, Michael A., Director, National Infrastructure Protection Center, Federal Bureau of Investigation before the Senate Armed Service Committee, Subcommittee on Emerging Threats and Capabilities, Washington, D.C., March 16, 1999".

Umstead, Thomas, "Tasks Force Outlines Stats, Initiatives", *Multichannel Online*, October 12, 1998.

Vatis, Michael A., Director, National Infrastructure Protection Center, Federal Bureau of Investigation before the Congressional Joint Economic Committee, Washington, D.C., March 24, 1998".

WarRoom Research, Inc. "Information Systems Security Survey", Annapolis Md., Nov. 1996.

WarRoom Research, Inc. "Corporate America's Security Intelligence Risk", Annapolis Md., 1998.

Wilson, Tim, "Profits Embolden Hackers", CMP Media, March 23, 1998

Yasin, Rutrell, "Hackers to Users, Feds: Internet is 30 Minutes from Disaster", CMP Media, 1998.

GLOSSARY

8K: eight thousand, where K or Kilo equals 1,000, as in 8K bytes, eight thousand bytes, or eight thousand characters, where each byte corresponds to one character (letter, number or special character). Also M, or Mega, equals 1,000,000 and G, or Giga, equals 1,000,000,000.

Bandwith: the data rate or speed of data through a network. Usually measured in bits per second (bps). A full page of English text is about 16,000 bits. A modem can move about 33,800 bits in one second (33.8 Kbps). Full-motion full-screen video would require roughly 10,000,000 bits-per-second (10Mbps), depending on compression.

Bit (Binary digIT) -- A single digit number in base-2, in other words, either a 1 or a zero. The smallest unit of computerized data. Bandwidth is usually measured in bits per second.

Circuit Board; "Board" : a composite board with attached microprocessors, memory chips and other components that are electrically connected through conducting paths on the board. The board is designed to be physically installed in a computer or other related device.

Browser: a client program (software) that requests and outputs web pages from a web server. These are the fundamental programs which allow access to the World Wide Web. Microsoft Internet Explorer and Netscape Communicator are typical examples.

Byte: a set of bits that represent a single character. Usually there are 8 bits in a byte.

Chip, Microchip: small modules that have computer memory or logic circuitry for microprocessors

Client: a software program that is used to contact and obtain data from a Server software program on another computer, often across a great distance. Each Client program is designed to work with one or more specific kinds of Server programs, and each Server requires a specific kind of Client. A "Web Browser" is a specific kind of Client.

Computer Virus: programming code, usually inserted in another program, that may result in some form of computer damage when executed. The most common form of viruses are written for Macros, scripts for Microsoft Word. Viruses that attach themselves to files and system software modules that are uploaded and executed cause the most damage.

Counterfeiting Software: the production of illicit copies of software programs (often on CD-ROMs), followed by packaging and selling the software as if it were a product normally sold by another company.

Database: a collection of data, organized in records with identical fields, so that its content can be accessed, updated and used in applications.

Denial of Service: various types of attempted accesses to a network which intentionally render it unable to function normally, either by loss or degradation of operational capability, such that the services to regular users are disrupted .

Digital Cash, or E-cash. a system of purchasing cash credits and transferring them electronically when making purchases over the Internet. Digital cash may also be stored on a smart card.

Smart Card: a plastic card, the size of a credit card, with an embedded microchip that can be loaded with data indicating a cash credit (surplus), and can be used to electronically pay for purchases. Smart cards can also exchange credits with other smart cards thus avoiding the need to transfer the money through a third party (i.e. a bank) and eliminating the possibility of recording or tracking the transfer.

Electronic Commerce; E-Commerce: the buying and selling of goods and services over the Internet, especially the WWW. E-Business also includes servicing customers and collaborating with business partners (as in business to business sales). Direct selling over the Internet is also known as E-tailing.

Electronic Data Interchange, EDI: a pre-Internet system of networked computer-to-computer exchanges of pre-formatted business transaction information, including purchases, payments and information exchange. Applications may also be linked between businesses using EDI standards. EDI functions are beginning to be replaced by electronic commerce over the Internet.

Electronic Mail, E-mail: messages, usually text, are placed on an server (e-mail server) with an e-mail application (e.g. Netscape, Internet Explorer, Eudora), sent to another server, based on its address, and are downloaded by an authorized recipient. E-mail can also be sent automatically to a large number of addresses (Mailing List).

Encryption: the encoding of data such that only the desired recipients can decode it. Encryption provides protection when transmitting sensitive data such as credit card numbers over a public network like the Internet.

Extensible Mark-up Language, XML: a flexible way to create common formats and to share the format and its related data on the WWW and elsewhere. It is similar to HTML and is seen as its replacement.

File: (1) a set or grouping of data such as some text, a digital graphic or a movie. Also, (2) a set of records where each record may have the same fields (e.g. name, age, etc.) although the values of the fields will differ.

Firewall: the hardware and/or software systems that separate one or more networks into two parts in order to protect an internal network system from the unauthorized intrusions of an outsider or to prevent insiders from exceeding their authorization. Sites may have firewalls within firewalls.

Computer Forensics: a methodical and thorough examination of computer media (hard disk drives, tape, diskettes and other portable media) for evidence of criminal activity.

Gray Market: unauthorized channels of product sales, where no warranties or standards are guaranteed for purchased products.

Hacker: In software circles, a hacker is a clever programmer. However, the news media currently uses the term hacker in a derogatory manner to refer to people that use their technical knowledge to gain unauthorized access and perform mischievous or destructive actions in networks and computer systems. Hacking is what a Hacker does.

High Tech Crime: Those crimes in which technology is used as an instrument in committing, or assisting in the commission of a crime, or which is the target of a criminal act.

HTML, HyperText Markup Language: a set of markup symbols, or tags, inserted in a file (of text, graphics, or other types of information) to be displayed that instruct the web browser how to display the information as a web page, that is, as a page on the WWW.

Information Technology, IT: encompasses all of the forms of technology used to create, store, exchange and use information in all of its forms.

Intellectual Property: property produced by the effort of the mind, such as unique ideas, that are protected from theft or unauthorized use by patent, copyright, trademark and trade secret law.

Internet, Net: a worldwide system of computer networks - a network of networks. A common protocol (TCP/IP, Transmission Control Protocol / Internet Protocol) allows internetworking of

communications; hence the name "Internet". The most widely used application on the Internet is electronic mail, or e-mail. The most widely used part of the Internet is the World Wide Web.

Interoperability: the ability of one system or product to work with another system or product without a special effort on the part of the user. Interoperability is based on interface standards.

Microprocessor: a computer processor on a microchip

Money Laundering: a process of depositing and electronically transferring money that conceals the true source of funds, such as criminal activity, and avoids taxes on these funds.

MP3, MPEG3 digitally compressed files: the record industry may lose substantial sums of money because of the unauthorized distribution of its copyrighted music over the Internet made possible by MP3 compression technology.

Network: A communications link between a source and a recipient of data. For example, when two or more computers are connected together to share resources,

Network or Computer Intrusion: Unauthorized access to a network or computer system; the first step in a range of high technology crimes.

Password: a protected word or string of characters that identifies or authenticates a user for access to a computer system, or a specific resource such as data set, file, or record.

Records: a set of data often comprised of subsets called fields.

Remarking: changing marked specifications of chips and other electronic components. The chips are sometimes physically altered to achieve faster than design speeds and soon burn out.

Router: a device or, increasingly, software that determines the next network point where a packet of data should be forwarded. The router may also translate between the operating systems of the networks to which it is connected.

Script, an interpreted program: a brief program or sequence of instructions, written in a language such as Perl, where each instruction is processed into machine language while the program is being executed. In a compiled program, all of the instructions are processed into machine language before the program is executed. Scripts are frequently used to forge links between software applications operating on the Internet.

Semiconductors: a material, such as silicon, that can conduct electricity under some conditions and not others and may be used to control electrical circuits (i.e. as a switch). Some impurities may be added to enhance the desired effect.

Server: (1) In general, a server is a computer program that provides services to other computer programs (clients) in the same or in other computers. (2) The computer that a server program runs in is also frequently referred to as a server (though it may contain a number of server and client programs). Specific to the WWW, a Web server is the computer program that serves, or provides, requested HTML pages or files as requested by a local, or client browser.

SET: Secure electronic transactions, a standard for safe e-commerce developed by Visa, MasterCard and others.

Sniffer: a software program that is installed to monitor network traffic. Sniffers may be used to collect logon and password information as it passes over the network.

Software Piracy: illegally copying and using a proprietary software program such as a commercial software product.

Spam; Spamming: inappropriate use a mailing list, to send unsolicited e-mail messages, usually advertisements.

TCP/IP, Transmission Control Protocol/Internet Protocol: a suite of protocols that defines the Internet. Originally designed for the UNIX operating system, TCP/IP software is now available for every major computer operating system.

Trade Secrets: Intellectual property that could cause significant loss to a company if disclosed to its competition.

Trap Door: Hidden code in a network that allows unauthorized access.

Trojan Horse: an apparently harmless program which when executed performs a valid function in the foreground, while a malicious set of instructions is initiated in background which are invisible to the user and may damage the user's system.

Uniform Crime Report: A system of crime statistics collection managed by the FBI.

Web Site; Site: A collection of related web pages located on a server and available to all with access to the WWW.

White-Collar Crime: crime attributed to employees, usually office workers. Typical examples are embezzlement and other forms of fraud.

World Wide Web; The Web; WWW: the universe of networked hypertext servers (HTTP servers) which allow text, graphics, sound files, etc. to be mixed together and presented on web pages.